CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6285.01C
DISTRIBUTION: A, B, C 15 May 2013

MULTINATIONAL AND OTHER MISSION PARTNER (MNMP) INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS

References: See Enclosure F.

1. Purpose. This instruction establishes a process to collect, validate, prioritize, and sustain operational requirements for Multinational and other Mission Partner Information Sharing systems as directed by the Department of Defense Instruction 8110.1 in reference a. It establishes the process for collection, assessment, prioritization and validation of new Information Sharing Capabilities, as well as requests for connection or improvement to existing Information Sharing Systems. Existing Information Sharing Systems covered by the instruction are listed in Enclosure D. The MNMP Information Sharing Requirements Management Process is established to serve as a single point of entry for all MNMP user requirements. New capabilities will be assessed for operational validation and passed to the appropriate organization for sponsorship through the Joint Capabilities Integration and Development System process. Requests for extension or improvement of existing Multinational Information Sharing (MNIS) systems will be validated and prioritized for alignment with programmed funding as required. The CJCSI 6285.01C process must remain aligned with guidance in DoDI 8110 and synchronized with the Mission Partner Environment (MPE) and Joint Information Environment (JIE) governance structures as they are developed.

2. Cancellation/Superseded. CJCSI 6285.01B, "Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process," Change 1, 13 September 2010, is hereby superseded.

3. Applicability. This instruction applies to Joint Staff, Combatant Commands (CCMDs), Services, Defense Agencies, and other DoD mission partner information sharing communities.

4. Guidance

a. The ability to share classified and unclassified information with allies and Coalition partners is a critical element in multinational/Coalition operations. Combined Enterprise Regional Information Exchange System (CENTRIXS), Pegasus (Griffin), SECRET Internet Protocol Router Network Releasable Demilitarized Zone (SIPRNet REL DMZ) and Unclassified Information Sharing Services (UISS) have provided proven classified and unclassified operational capabilities and services; and the Combined Federated Battle Laboratories Network (CFBLNet) provides a valuable coalition research, development, test, and assessment environment. These operational and direct support networks/systems may be included in DoD efforts to improve mission partner information sharing and effectiveness.

b. The process defined in this instruction integrates CCMD, Service, agency, and mission partner priorities across all phases of military operations (Shape the Environment, Deter the Enemy, Seize the Initiative, Dominate the Enemy, Stabilize the Environment, Enable Civil Authority) and provides procedures for allies, mission partners, and other participating nations to identify and address interoperability considerations affecting existing operational and direct support systems. Requirements will be submitted at any time via the Joint Staff J-6 Net-enabled Requirements Identfication Database (NRID) on SIPRNet (http://intelshare.intelink.sgov.gov/sites/nrid) per the procedures in the NRID Quick-Help Guide. The J-8 sponsored Knowledge Management and Decision Support (KMDS) System will continue to be used to manage Joint Capabilities Integration and Development System (JCIDS) documents for JROC validated capabilities and requirements. The Intelligence Community (IC) Capability Requirements (ICCR) process will continue to be used for IC requirements.

c. CCMDs, Services, and agencies will submit all MNMP Information Sharing requirements through the Joint Staff submission process with an operational endorsement from the submitting organization's J-3 or equivalent operational entity. Requirements will be submittted using the template at Enclosure C and the checklist in Enclosure F. Mission critical requirements will be accepted for immediate adjudication and validation through the out-of-cycle process outlined in Enclosure B (Figure 2). Mission essential requirements may be accepted for immediate adjudication and validation through the out-of-cycle process dependent on the criteria in paragraph 4.d (ii)(3) below. Mission enhancing requirements for an extension of or improvement to existing MNIS information sharing capabilities will be consolidated quarterly for validation and prioritization by the Joint Staff J-3 and resourced appropriately utilizing the process outlined in Enclosure B (Figure 1).

d. CCMDs, Services, agencies, and the Joint Staff apply the following categorization criteria when submitting and prioritizing MNMP requirements.

(1) Priority 1: Mission Critical

(a) Failure to satisfy the requirement will result in extreme risk or high probability of catastrophic consequences (such as mission failure, potential loss of life or severe injury, or severe damage to property).

(b) No work-arounds or alternative solutions exist.

(c) Capability is needed immediately to mitigate risk.

(2) Priority 2: Mission Essential

(a) Failure to satisfy the requirement will significantly degrade or prevent an organization from accomplishing its mission.

(b) No acceptable work-arounds or alternative solutions exist.

(c) Requirement is needed not later than a specific date to prevent loss/degradation of capability.

(3) Priority 3: Mission Enhancing

(a) Requirements that will improve/enhance an organization's ability to execute its assigned mission.

(b) Capability is needed as soon as possible.

e. As required, the C4/Cyber Functional Capabilities Board (C4/Cyber FCB), in coordination with other relevant capability boards (e.g., Battlespace Awareness, Logistics, Force Application, Force Protection) will assess MNMP information sharing capability requirements against competing priorities and constraints to determine the best resource strategy.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. Redefined scope of instruction. Ensured all DoDI 8110.1 guidance, authorities and responsibilities for the Joint Staff were adequately addressed. Updated the MNMP requirements categorization and prioritization criteria. Updated MNMP requirements process flow diagram. Added requirements out-of-cycle management process flowchart. Updated responsibilities at Enclosure A.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DoD Components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

10. This instruction will be reviewed and updated as required following any changes to DoDI 8110.

For the Chairman of the Joint Chiefs of Staff

CURTIS M. SCAPARROTTI
Lieutenant General, U.S. Army
Director, Joint Staff

ENCLOSURES:

A – RESPONSIBILITIES
B – MNMP INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS FLOW CHART
C – MNMP REQUIREMENTS REQUEST FORMAT TEMPLATE
D – EXISTING MNIS INFORMATION SHARING CAPABILITIES
E – MATRIX/CHECKLIST OF AGREEMENTS, AUTHORITIES, POLICIES
F – REFERENCES
GL – GLOSSARY OF DEFINITIONS

ENCLOSURE A

RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff (CJCS) serves as primary focal point for collecting, adjudicating, prioritizing, and validating MNMP requirements and providing them to the appropriate Service or agency for proper planning, engineering, and execution. All MNMP requirements will be addressed utilizing the appropriate process flow chart at Enclosure B. The process will ensure interoperability, integration, compatibility, prioritization, and consistency of requirements across requesting CCMDs, Services, and agencies.

a. The Joint Staff J-6 will:

(1) Provide oversight of the entire MNMP requirements management process.

(2) Consolidate CCMDs, Services, and agencies requirements quarterly to capture new and revalidate existing MNMP requirements.

(3) Accept and process out-of-cycle mission critical/essential MNMP requirements that must be met prior to the next quarterly requirements consolidation and prioritization.

(4) Ensure CENTRIXS Connection Requests (CCRs) submitted via the Defense Information Systems Agency (DISA) Enclave Connection Approval Process (ECAP) do not delay or defer existing MNIS requirements validated by this process. Connection requests that will delay or defer existing C4/Cyber FCB approved requirements efforts must be submitted via the CJCSI 6285 process outlined in Enclosure B for Joint Staff J-3 prioritization.

(5) Determine and assign a requirements document sponsor (supported/lead) organization, as needed.

(a) Services and the Joint Staff may sponsor requirements for capabilities that span multiple CCMDs, Services or agencies and will assume the responsibilities outlined on page A-5.

(b) Requirements supporting Multinational or other Mission Partners must be sponsored by a U.S. DoD organization.

(6) Review MNMP requirements submissions for completeness and clarity and conduct meetings with CCMDs, Services, agencies, DISA, Joint Staff, and customer stakeholders as required to clarify content of submissions, ensure they fit into the MNIS portfolio, and determine suitability for continued processing. Suitable requirements are those requesting improvement to or

extension of an existing capability. New capability requirements are not considered suitable for this process and will be assessed for potential submission via the JCIDS requirement process or inclusion in an existing Program of Record (see instructions in Enclosure B).

(7) Convene appropriate functional requirements area working groups (Classified Information Sharing Services (CISS), UISS or CFBLNet) to enable proper vetting for requirement acceptability. An acceptable requirement meets current policy, security and regulatory guidelines. CISS working groups will have at a minimum the following stakeholders represented: OSD (Policy), USD (Intelligence) Foreign Disclosure, CYBERCOM, DISA, DoD CIO, and Defense Information Systems Network (DISN) Flag Panel (Defense Security Accreditation Working Group (DSAWG)). The UISS working groups will have at a minimum the following stakeholders represented: Joint Staff, CCMDs, and DISA.

(8) Vet and endorse CCMD, Service, and agency out-of-cycle resourced MNMP requirements not requiring DISA support (funding/labor).

(9) Consolidate and forward MNMP requirements to Joint Staff J-3 for prioritization.

(10) Present the Joint Staff J-3 prioritized MNMP requirements to the C4/Cyber FCB for approval.

(11) Coordinate recommended resource strategy, to include roles and responsibilities, technical solution, implementation plan/schedule and cost estimates, with requirements document sponsor and the Joint Staff J-3.

(12) UISS, CISS, and CFLNet working groups will coordinate with the C4/Cyber FCB to assess requirements against competing priorities and constraints to determine the best approach. Following initial review by Joint Staff J-6, suitable Unclassified MNMP information sharing requirements will be forwarded to the UISS Working Group for acceptability review. Acceptable requirements will be forwarded to the Joint Staff J-3 for validation/prioritization. Joint Staff J-6 will ensure proper adjudication, vetting, validation, and prioritization of unclassified domain requirements in accordance with the management process flow charts in Enclosure B. Joint Staff J-6 will coordinate directly with customer stakeholders for further clarification or work on any Joint Staff J-3 recommended decision to not validate a requirement.

(13) Present final resourcing strategy, to include roles and responsibilities, technical solution, implementation plan/schedule, cost estimates, and recommended funding strategy, to the C4/Cyber FCB for approval and provide final results to the requirement document sponsor.

Facilitate follow-on activities to address customer request for reprioritization or shift of resources to satisfy requirements.

(14) Endorse mission critical/essential requirements whose resource strategies, costs and implementation plan, will not delay or defer DISA effort to meet current requirements. Forward requirements that will delay or defer DISA efforts to implement/execute existing C4/CYBER FCB validated requirements to the Joint Staff J-3 for prioritization.

(15) Update the C4/Cyber FCB monthly on status of MNMP requirements (existing and out-of-cycle).

(16) Maintain a permanent standing database of validated resourced (funded and/or executed) and unresourced requirements, plus associated procedures.

c. The Joint Staff J-3 will:

(1) Validate and prioritize MNMP requirements and forward to Joint Staff J-6 for further processing.

(2) Approve J6 recommendations for requirement category and out-of-cycle acceptance for processing.

(3) Return all requirements not accepted for out-of-cycle processing to the sponsor organization via a letter of nonconcurrence.

(4) Re-prioritize MNMP requirements when out-of-cycle submissions will delay or defer DISA's ability to resource, implement/execute existing C4/Cyber FCB validated requirements.

(5) Apply the following suggested prioritization criteria to ensure available resources are equitably distributed throughout the Warfighting Community.

(6) Requirement Category:

(a) Mission Critical

(b) Mission Essential

(c) Mission Enhancing

(d) Type of Supported Mission:

1. Operations: Capability supports units whose mission involves direct engagement with enemies or mission partners across the spectrum of operations.

2. Operations Support: Capability supports units whose mission involves communications or intelligence support of organizations directly engaged with enemies or mission partners.

3. Sustainment: Capability supports units whose mission involves sustainment of forces (functional areas such as administration and logistics).

(7) Scope of capability:

(a) Provides capability across the entire DISN Enterprise.

(b) Supports multiple CCMDs, Services, agencies or Organizations.

(c) Supports a single CCMD, Service, agency or Organization.

(d) Size of supported Organization

(8) Duration of Requirement: Enduring or Temporary (e.g., Exercise)

(9) Type of capability required.

d. C4/Cyber FCB will:

(1) Provide oversight and final decision authority for MNMP capabilities requirements evaluation, advocacy, and support for CCMDs, Services, and agencies.

(2) Coordinate and align MNMP requirements with other Capability Board(s) (as required).

(3) Approve Joint Staff J-3 prioritized MNMP requirements and forward to the appropriate Service or agency for a recommended resourcing strategy, to include roles and responsibilities, technical solution, implementation plan/schedule, and cost estimates.

(4) Approve resourcing strategies presented to the C4/Cyber FCB.

e. DISA will:

(1) Manage MNIS requirements programming and budgetary activities in support of Warfighter operational requirements. Actively participate in the OSD Program Objective Memorandum (POM) process, to include providing POM estimate for funding to satisfy the current unfunded MNIS operational

requirements and migration of the MNIS operational system capabilities to an enterprise level.

(2) Upon FCB approval of validated and prioritized MNMP requirements, coordinate directly with customer stakeholders, and provide a recommended resourcing strategy, which includes technical solutions, SME support, implementation plan/schedule, costs and requirements that can be met with existing resources to Joint Staff J-6 for staffing.

(3) Based on CCMD, Service, and agency funding input, update final recommended resourcing strategy appropriately. Upon C4/Cyber FCB approval of final resourcing strategy, execute implementation plan, as required, to satisfy operational requirement.

(4) Ensure solutions to the MNMP requirements are appropriately integrated with current DoD Information Networks (DoDIN) and Network Operations (NETOPS) policies. In conjunction with the Joint Staff J-6, determine where migration of the MNIS capabilities to an enterprise services level is appropriate and implement that migration within programmed funding constraints.

(5) Coordinate with other CCMDs, Services, and agencies, as required, to satisfy planning, engineering and execution of applicable MNMP requirements.

f. Combatant Commands, Services, and agencies will:

(1) Submit MNMP requirements to Joint Staff J-6 through the process outlined in this instruction via NRID-S. If the Web site is down or the submitter is having technical difficulties, the requirement may be submitted via e-mail following the format in Enclosure C.

(2) Review the recommended technical solutions, and costing and implementation schedules, and determine if your command, Service, or agency is willing to fund unresourced MNMP requirements or defer the requirement. Provide your response to the Joint Staff J-6.

(3) Be responsible for funding user workstations or terminals, as well as the supporting network transport infrastructure from the Defense Information Systems Network (DISN)/DoDIN/CMNT Point of Presence (POP) to the Customer Edge and beyond.

(4) Ensure local operational commanders are authorized to extend their operational systems(s)/network(s) and/or add workstations as long as it does not require establishing a new POP within their AOR. The local commanders must ensure that all pertinent safeguards and procedures are addressed and

reported to the local information manager. External resources will not be provided to support the above extension and/or additional workstation(s).

(5) Comply with all references, related processes, publications and policies listed in Enclosure D when submitting requirements. Examples enforced by the C4/Cyber FCB include but are not limited to Multinational Information Sharing Agreements, Communications Interoperability and Security Memorandum of Agreements (CIS MOAs), International Agreements, General Security of Military Information Agreement (GSOMIA) and Technical Implementation Agreement/Arrangement.

(6) Inform Joint Staff J-6 of version changes for approved capabilities via the NRID. A new CJCSI 6285.01C request is not needed for version updates. For example, on CX-I an update from C2PC version 6.1.1 P4 to version 7.0.3.1 does not require a new CJCSI 6285.01C request.

ENCLOSURE B

MNMP INFORMATION SHARING REQUIREMENTS MANAGEMENT PROCESS FLOW CHART

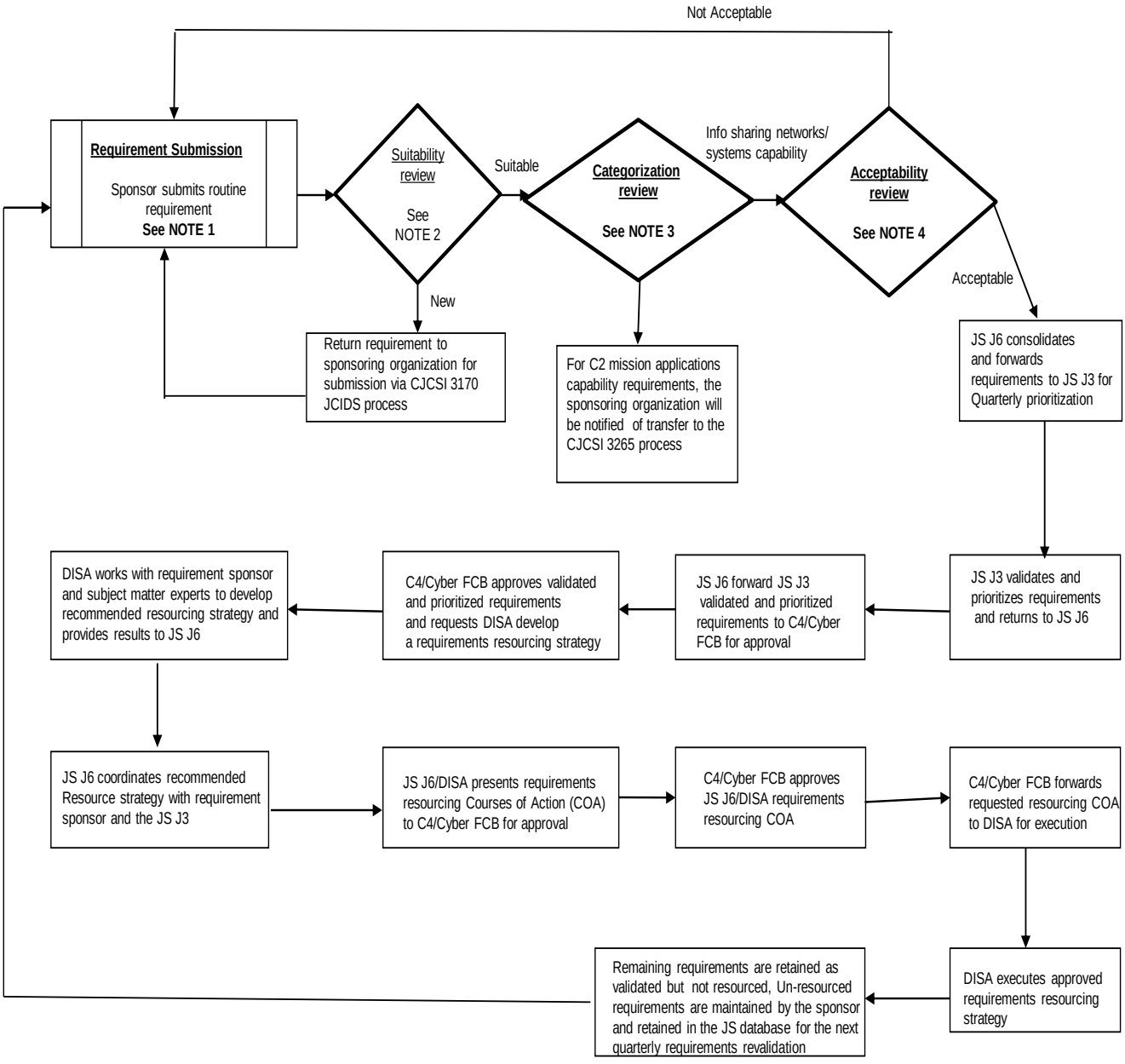

Figure 1. MNMP Information Sharing Process Flow Chart

FIGURE 1 NOTES

1. **Note 1**: MNMP requirements may be submitted to the Joint Staff J-6 at any time via http://intelshare.intelink.sgov.gov/sites/nrid. Routine requirements will be consolidated and forwarded to Joint Staff J-3 for prioritization quarterly and addressed within 90 days. Requirements are maintained by the sponsor and retained in the Joint Staff permanent standing database until met or withdrawn by the sponsor.

2. **Note 2**:

a. Joint Staff J-6 conducts review with requirements sponsor and subject matter experts to determine if the requirement is suitable for processing via CJCSI 6285. Suitability and unsuitability are defined as:

(1) Suitable: The requirement constitutes an extension of, or improvement to an existing capability (.e.g., a request to extend a Point of Presence of an existing MNMP network or secure voice for a coalition operation).

(2) Unsuitable: Requests for new capabilities not currently existing within the Portfolio of systems listed in Enclosure E to this instruction (.e.g., a request to establish a new CENTRIXS network).

b. Requests for new capabilities that are unsuitable for processing within CJCSI 6285, the sponsoring organization would be notified that the requirement has been transferred to the appropriate process (CJCSI 3170 JCIDS or CJCSI 3265 Mission Applications).

3. **Note 3**: MNMP requirements categorization review will distinguish between command and control (C2) mission applications and information sharing networks/systems capabilities. C2 mission application capability requirements will be returned to the sponsoring organization for submission via CJCSI 3265 process.

4. **Note 4**: Suitable requirements are assessed for acceptability by an appropriate functional area working group (CISS/UISS/CFBLNet). Requirements are considered acceptable if they meet current security, regulatory and policy standards. If needed, requirements are sponsored through the Defense Security Accreditation Working Group (DSAWG) and DISN Flag Panel for approval. Requirements considered unacceptable will be returned to the sponsoring organization for further assessment, and are afforded the opportunity to pursue policy change if desired.

MNMP INFORMATION SHARING REQUIREMENTS OUT-OF-CYCLE MANAGEMENT PROCESS FLOW CHART

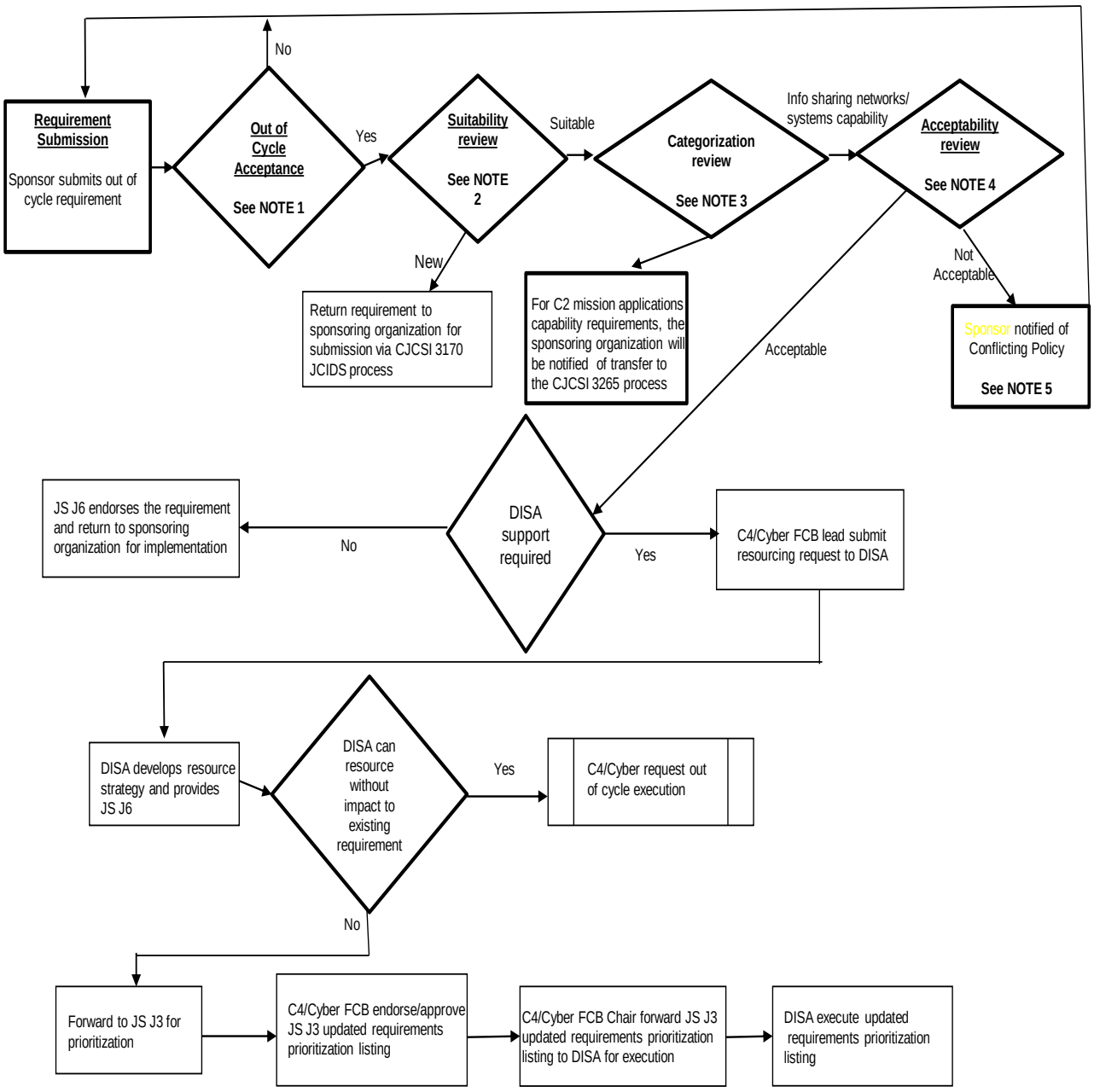

Figure 2. MNMP Information Sharing Out-Of-Cycle Process Flow Chart

FIGURE 2 NOTES

1. **Note 1**: Joint Staff J-6 coordinates with Joint Staff J-3 to determine if requirement meets out-of-cycle criteria.

(a) All Mission Critical Requirements will be accepted as out-of-cycle.

(b) Mission Essential Requirements that must be met before the next routine quarterly validation and prioritization will be accepted as out-of-cycle.

(c) Requirements not accepted as out-of-cycle will be returned to the sponsor with a letter of non-endorsement from the J-3, and may be processed as a routine requirement.

2. **Note 2**: Mission Critical/Essential requirements will be assessed against the same suitability criteria defined above for in-cycle requirements. Requirements determined to be unsuitable will be returned to the sponsoring organization for submission via CJCSI 3170 JCIDS process.

3. **Note 3**: Mission Critical/Essential requirements will be assessed against the same categorization criteria defined above for in-cycle requirements.

4. **Note 4**: Mission Critical/Essential requirements will be assessed against the same acceptability criteria defined above for in-cycle requirements. Requirements that fall into the MNIS portfolio will be forwarded to DISA for support.

5. **Note 5**: Commanders of requesting (sponsoring) organizations must be given immediate opportunity to engage with Joint Staff and DoD Senior Leadership if desired to request exception to Policies that conflict with Mission Critical requirements.

ENCLOSURE C

MNMP REQUIREMENTS REQUEST FORMAT TEMPLATE

CJCSI 6285 Request Template: Multinational and Other Mission Partner Information Sharing Requirements Request

A. Mission Impact (Mission Critical, Mission Essential, Mission Enhancing):

B. Operational Requirement: State the operational requirement and capability (e.g., Require a radio gateway connection to CENTRIXS ISAF (CX-I) that provides an interconnection between various sets of radio networks allowing secure, tactical, real-time, high fidelity video, data and voice services to be deployed in a networked environment to support tactical operations.) **Do not identify solution (s)**.

C. Capability Need Description: Detailed description of operational capability; operational gaps/shortfall requirement will address; and mission criticality (critical, essential, enhancement). Link operational shortfall to Joint Urgent Operational Needs Statement, (JUONS), Operational Needs Statement (ONS) and/or Initial Capability Document (ICD). Examples of operational gaps/shortfalls include (a) nonexistent or limited use of C2 services in a Disconnected Intermittent or Low (DIL) bandwidth environment, (b) limited ability to maintain and share SA while On The Move (OTM), (c) lack of ability for leaders to provide accurate and timely guidance and intent of Coalition Forces (CF) and Afghan National Security Forces (ANSF) mission partners while OTM, and (d) inability to collaborate OTM.

D. Justification:

1. Impact to mission if requirement not met

2. Expected Benefits

3. Workarounds in place

E. Operational Endorsement: Attach a separate memorandum signed by your operations shop (O-6 and above)

F. Submitter's Contact Information:

G. Submitter's Supervisor Contact Information:

H. Requirement Point of Contact Information (applicable stakeholders):

I. Type of capability: New capability; sustainment of, extension of or improvement to an existing capability

J. Interoperability: Fully interoperable and compatible with current, as well as future, international standards (i.e., IPV6) and legacy systems currently in use (e.g., CENTRIXS family of systems).

K. Service/Agency-Managed Systems the solution must be compatible with: (e.g., Theater Battle Management Core System (TBMCS), or Battle Command Common Services (BCCS).

L. Responsibility for Requirement costs (e.g., design, implementation and sustainment): (Customer, DISA, N/A)

M. Training Requirements:

N. Additional Human Resources Required:

O. Logistics Support (e.g., CJCSI 6510.06 Series, "Communications Security Releases to Foreign Countries"):

P. Capability Categorization: Command and Control mission application; Information Sharing network/system

Q. CCMD/Service/Agency Priority: (e.g., #1 of 5)

R. Brief History of Previous Submission(s):

S. Additional Comments:

ENCLOSURE D

EXISTING MNIS INFORMATION SHARING CAPABILITIES

1. Combined Enterprise Regional Information Exchange System (CENTRIXS): Defined as all existing CENTRIXS enclaves and efforts to improve CENTRIXS capabilities such as the Common Mission Network Transport (CMNT) initiative.

2. Pegasus (Griffin): Pegasus (not an acronym) is the Combined Communications and Electronics Board led effort to improve and increase current (Griffin) collaborative services available between FVEY national Secret networks.

3. Secret Internet Protocol Router Network (SIPRNet) Releasable (REL) Demilitarized Zone (DMZ): Defined as all U.S. SIPRNet enclaves extended to enable FVEY partner access to Secret-Releasable information.

4. Combined Federated Battle Laboratory Network (CFBLNet): Provides the infrastructure of choice for international Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) research, development, trials and assessment to explore, promote and confirm MNMP capabilities.

5. Unclassified Information Sharing Services (UISS): The UISS is a shared enterprise service to facilitate unclassified information sharing with mission partners that do not have or want access to DoD networks or Web portals.

(INTENTIONALLY BLANK)

ENCLOSURE E

MATRIX/CHECKLIST OF AGREEMENTS, AUTHORITIES, POLICIES

Below is a matrix/checklist of information sharing references (agreements, authorities and policies) that CCMDs, Services, and agencies must address prior to submitting a 6285 requirements document. This front loaded guidance for customers will streamline the appropriate requirements working group's efforts by arming the customers with information sharing expectations from a policy, security and operational/technical perspective.

COUNTRY	INTERNATIONAL AGREEMENT (DoDD 5530.3)	CONPLANS/ OPORD (Command)	CISMOA (CJCSI 6510)	GSOMIA (NDP-1)	TECHNICAL AGREEMENT (DoDD 5530.3)	EXCEPTIONS TO NATIONAL DISCLOSURE POLICY (NDP-1)	Foreign Military Sales/National/ Multi-Fora Agreements
X	Type of Information Exchange Agreement	XXXX-XX	Authority to transfer COMSEC hardware/ software	Agreement for the protection of classified material	Country COMSEC support agreement	General information sharing specifics	Additional Agreements

(INTENTIONALLY BLANK)

ENCLOSURE F

REFERENCES

a. DoDI 8110.1, 6 February 2004, "Multinational Information Sharing Networks Implementation"

b. CJCSI 3170.01 Series, "Operation of the Joint Capabilities Integration and Development System"

c. JROCM 042-06, 20 March 2006, "MNIS Way Ahead"

d. Combined Enterprise Regional Information Exchange System (CENTRIXS) Operational Need Statement (ONS), 27 April 2005

e. Globally Reaching Interactive Fully Functional Information Network (Griffin) Operational Need Statement (ONS), 27 April 2005

f. Combined Federated Battle Laboratory Network (CFBLNet) Operational Needs Statement (ONS), 27 April 2005

g. DoDI 8910.01, 6 March 2007 (CH-1 incorporated 17 January 2013), "Information Collection and Reporting"

h. NDP-1, National Disclosure Policy and Procedures for the Disclosure of Classified Information to Foreign Governments and International Organizations,1 October 1988

i. DoDI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSSI)"

j. CJCSI 6212.01 Series, "Net Ready Key Performance Parameters (NR KPP)"

k. CJCSI 6510.06 Series, "Communications Security Releases to Foreign Countries"

l. CJCSI 3265.01 Series, "Command and Control Governance and Management"

m. DoDI 8410.02, December 2008, "NetOps for the Global Information Grid (GIG)"

n. DoD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

o. DoD Directive 5530.3, 11 June 1987 (Certified current as of 21 November 2003), "International Agreements"

p. U.S., CCEB, NATO, "CFBLNet Publication 1", 30 October 2009, at http://www.disa.mil/cfblnet/index.html "access: date 19 August 2012

ENCLOSURE G

GLOSSARY OF DEFINITIONS

1. Combined Communications Electronics Board (CCEB). A five-nation joint military communications-electronics (C-E) organization whose mission is the coordination of any military C-E matter that is referred to it by a member nation. The CCEB member nations are Australia, Canada, New Zealand, the United Kingdom, and the United States. The CCEB Board consists of a senior C4 representative from each member nation.

2. Combined Enterprise Regional Information Exchange System (CENTRIXS). CENTRIXS is a common set of networks built on a set of standard hardware, software, and services for U.S. and Coalition partner forces to share classified operational and intelligence information at the SECRET/REL level. Each of these CENTRIXS networks operates at a single security classification level and operates globally, regionally, and locally.

3. Combined Federated Battle Laboratories Network (CFBLNet). A laboratory environment which utilizes a distributed Wide-Area Network used as the vehicle for network members (Combined Communications Electronics Board and NATO), to experiment with new capabilities by conducting Research and Development, Trials and Assessment (RDT&A) initiatives.

4. Common Mission Network Transport (CMNT). Enterprise backbone infrastructure that will allow CCMD/Service/agency(s) to exchange and share information across regional operational network domains via the Defense Information System Network (DISN) backbone architecture without tunneling through layers of various transport. CMNT will provide a common transport for encrypted CENTRIXS traffic to meet mission partner information sharing requirements.

5. Defense Information Systems Agency (DISA). A Combat Support Agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, national level leaders, and other mission and Coalition partners across the full spectrum of operations.

6. Department of Defense Information Networks (DoDIN). The globally interconnected, end-to-end set of information capabilities, associated process and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers, and support personnel. The DoDIN includes owned and leased communications and computing

systems and services, software (including applications), data, security services, other associated services, and National Security Systems.

7. Enterprise Network. As designated by the DoD CIO Executive Board, a network that provides a defined capability; is available to serve multiple DoD Components; complies with the DoDIN architecture; is managed with Enterprise-wide oversight; and provides service to any user with a validated requirement.

8. Functional Capabilities Board (FCB). FCBs are established bodies that are part of the Joint Capabilities Integration and Development System (JCIDS). They are responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area.

9. Griffin. A collection of networks and services that enable e-mail capability between the national systems of participating nations.

10. Joint Information Environment (JIE). A framework to synchronize and integrate C4ISR capabilities and services delivered through a shared, secure GIG using standardized guidance designed to achieve the decisive information advantage for the Warfighter. It is comprised of shared information technology infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies.

11. Mission Partner Environment (MPE). A mission partner operating environment that leverages U.S. and mission partner information technology infrastructures with integrating capabilities to realize the DoD JIE framework.

12. Multinational Information Sharing (MNIS). A collection of net-centric applications and services capabilities that shall be resident in the future Enterprise Information Environment (EIE) of the DoDIN and shall function as an MNIS Community of Interest (COI) interfaced through the appropriate NSA developed and accredited information assurance cross domain solutions to allow for unfettered sharing of MNIS information at SECRET and below levels with foreign nations and forces as an integrated MNIS solution to support the combined warfighting environment. MNIS shall include the acquisition and integration of those MNIS COI services and applications into the DoDIN.

13. Pegasus. A CCEB managed program to improve collaborative services and information sharing capability between FVEY nations by connecting national-to-national SECRET network services through gateway proxy servers. The program includes improved National Secret E-mail capability, Web Browsing, Chat, and Internet Protocol (IP) Video Teleconferencing.

14. SIPR REL DMZ. The primary objective of the SIPR REL network is to provide a consistent, sustainable, secure environment to share real time, mission-valued information through reliable and controlled access to SIPRNet Web sites to authorized Coalition partners while maintaining the security and integrity of the SIPRNet. The overall SIPR REL network provides several services that enable information sharing between U.S. SIPRNet users and foreign national/exchange officers embedded in U.S. enclaves and in enclaves located in partner countries.

15. Unclassified Information Sharing Services (UISS). UISS provides structured (e.g., file sharing and calendaring) and unstructured (e.g., wikis, blogs, and forums) collaboration capabilities to the enterprise for the purposes of unclassified information sharing with multinational partners, non-governmental organizations, the various U.S. Federal and State agencies, and members of the public and private sectors. Capability enables effective information exchange and collaboration between the United States Department of Defense (DoD) and any external country, organization, agency or individual that does not have ready access to traditional DoD systems and networks. These mission partners include, but are not limited to, U.S. government agencies; foreign governments and their militaries; international organizations (IOs); regional organizations (ROs); nongovernmental organizations (NGOs); State, local and tribal authorities; and members of the public and private sectors. It enables professional networking and communication, increases situational awareness, establishes pre-defined communications channels, relationships and information workflows, and provides a forum for sharing lessons learned and best practices in a wide variety of contexts including crisis response, humanitarian assistance, disaster relief, training, and exercises.

(INTENTIONALLY BLANK)